Math 100: Problem Set 4

Owen Jones

11/1/2023

(Q-1) We can express the number 1 written $p-1$ times as $\sum_{k=0}^{p-2} 10^k$. It follows $\sum_{k=0}^{p-2} 10^k = \frac{10^{p-1}-1}{10-1}$. By Fermat's Little Theorem $10^{p-1} \equiv 1 \mod (p)$, so p divides $10^{p-1}-1$. Therefore, p must divide either $\sum_{k=0}^{p-2} 10^k$ or 9. p is a prime greater than 3, so p can't divide 9. Thus, p must divide $\sum_{k=0}^{p-2} 10^k$.

(Q-2) Since $\gcd(2, 121) = 1$, we can use Euler's Theorem to show $2^{\phi(121)} \equiv 1 \mod (121)$. $\phi(121) = 121(1 - \frac{1}{11}) = 110$ because 121 is relatively prime to every number up to itself except for multiples of 11. Thus $2^{998} = 2^8 2^{9\phi(121)} \equiv 2^8 \mod (121)$. $2^8 = 256 = 2 \cdot 121 + 14 \Rightarrow 2^{998} = 14 \mod (121)$.

(Q-3) $p^{5-1} \equiv 1 \mod (5), p^{3-1} \equiv 1 \mod (3)$, and $p^{\phi(16)} \equiv 1 \mod (16)$ by Euler's Theorem. It follows $p^{2(5-1)} \equiv 1 \mod (5), p^{4(3-1)} \equiv 1 \mod (3)$, and $\phi(16) = 16(1 - \frac{1}{2}) = 8$. Therefore $p^8 - 1$ is divible by $3, 5$, and 16. Since $3, 5$, and 16 are all relatively prime, $p^8 - 1$ must be divisible by their product, 240.

(Q-4) We want to use the Euclidean Algorithm.

$$\begin{aligned}
x^8 - 1 &= x^3(x^5 - 1) + x^3 - 1 \\
x^5 - 1 &= x^2(x^3 - 1) + x^2 - 1 \\
x^3 - 1 &= x(x^2 - 1) + x - 1 \\
x^2 - 1 &= (x+1)(x-1)
\end{aligned}$$

This implies

$$\begin{aligned}
(x^3-1)-x(x^2-1) &= x-1\\
(x^8-1-x^3(x^5-1))-x(x^5-1-x^2(x^3-1)) &= x-1\\
x^8-1-(x^3+x)(x^5-1)+x^3(x^3-1) &= x-1\\
x^8-1-(x^3+x)(x^5-1)+x^3(x^8-1-x^3(x^5-1)) &= x-1\\
(x^3+1)(x^8-1)-(x^6+x^3+x)(x^5-1) &= x-1
\end{aligned}$$

Thus, we choose $F(x) = x^3+1$ and $G(x) = -x^6-x^3-x$

(Q-5) Let $P(x) = x^{4a}+x^{4b+1}+x^{4c+2}+x^{4d+c}$ and $Q(x) = x^3+x^2+x+1$. We can express $P(x) = A(x)Q(x)+R(x)$ where $A(x)$ and $R(x)$ are polynomials and $R(x)$ has degree less than $Q(x)$.
$P(i) = i^{4a}+i^{4b}i+i^{4c}i^2+i^{4d}i^3 = 1+i+i^2+i^3 = 1+i-1-i = 0$
$P(-i) = (-i)^{4a}+(-i)^{4b}(-i)+(-i)^{4c}(-i)^2+(-i)^{4d}(-i)^3 = 1-i-1+i = 0$
$P(-1) = (-1)^{4a}+(-1)^{4b}(-1)+(-1)^{4c}(-1)^2+(-1)^{4d}(-1)^3 = 1-1+1-1 = 0$
$P(x) = Q(x)$ at three different points, so $R(x) = 0$ at those three points. However, the only polynomial of degree less than 3 that has more than 2 roots is the zero function. Thus $Q(x)$ is a factor of $P(x)$

(Q-6) (a) $x^8+x^4+1 = x^8+2x^4+1-x^4$
$= (x^4+1)^2-(x^2)^2$
$= (x^4-x^2+1)(x^4+x^2+1)$

(b) $(x^4-x^2+1)(x^4+x^2+1) = (x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1)(x^2+x+1)(x^2-x+1)$

(c) $(x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1)(x^2+x+1)(x^2-x+1) = (x+\frac{\sqrt{3}-i}{2})(x+\frac{\sqrt{3}+i}{2})(x-\frac{\sqrt{3}-i}{2})(x-\frac{\sqrt{3}+i}{2})(x-\frac{1+\sqrt{3}i}{2})(x-\frac{1-\sqrt{3}i}{2})(x+\frac{1+\sqrt{3}i}{2})(x+\frac{1-\sqrt{3}i}{2})$

(Q-7) (a) Let $f(x)$ have the rational root $\frac{p}{q}$. It follows by Gauss' Lemma that $f(x) = (qx-p)a(x)$ for some polynomial $a(x)$ with integer coefficients. We are given that $f(1)$ is odd, so $(q-p)$ must be odd and $a(1)$ must be odd. It follows that p and q have different parity. However, this means that $p \nmid a_0$ or $q \nmid a_n$ because an odd number can't be divisible by an even number. Thus, we obtain a contradiction, so $f(x)$ has no rational roots.

(b) $x^{13}+x+90 = f(x)(x^2-x+a)$ for some polynomial with integer coefficients. Observe $1^{13}+1+90-0^{13}-0-90 = 2 = a(f(1)-f(0))$. Thus, a divides 2. It follows $a = \pm 1, \pm 2$. WTS $x^2-x+2|x^{13}+x+90$ By long division $x^{13}+x+90 = (x^11+x^10-x^9-3x^8-x^7+5x^6+7x^5-3x^4-17x^3-11x^2+23x+45)$

(Q-8) (a) We will show both directions by induction. Let $F(x)$ be a polynomial. For the forward direction, we assume a is a zero multiplicity of $m+1$.

$P(0)$: If a is a zero multiplicity of 1 then let $F(x) := (x-a)B(x)$ where $B(x)$ is a polynomial that is nonzero at $x = a$. Because a is a root $F(a) = 0$, but $F'(a) = B(a) + (a-a)B'(a) = B(a) \neq 0$. Thus, $P(0)$ holds.

$P(m)$: Assume $F^{(i)}(a) = 0$ for $0 \leq i \leq m$ and $F^{(m+1)}(a) \neq 0$ for some m.

$P(m+1)$: Let $F(x) := (x-a)^{m+2}B(x)$ where $B(x)$ is a polynomial that is nonzero at $x = a$.

$F(a) = 0$ because a is a root. $F'(x) = (m+2)(x-a)^{m+1}B(x) + (x-a)^{m+2}B'(x)$

$= ((m+2)B(x) + B'(x)(x-a))(x-a)^{m+1}$

Because $(m+2)B(a) + B'(a)(a-a) \neq 0$, a is a zero multiplicity of $m+1$ for $F'(x)$, so by the induction hypothesis $F^{(i+1)}(a) = 0$ for $0 \leq i \leq m$ and $F^{(m+2)}(a) \neq 0$. Hence, by induction, the claim holds for all m

For the reverse direction, we assume $F^{(i)}(a) = 0$ for all $0 \leq i \leq m$.

$P(0)$: $F(a) = 0 \Leftrightarrow a$ is a root of $F(x)$. Thus, we can define $F(x) := (x-a)B(x)$. $F(a) = (a-a)B(a) = 0$. $F'(x) = B(x) + (x-a)B'(x)$ and $F'(a) \neq 0$, so a is not a root of $B(x) \Rightarrow a$ is a zero multiplicity of 1.

$P(m)$: If $F^{(i)}(a) = 0$ for all $0 \leq i \leq m$ assume a is a zero multiplicity of $m+1$.

$P(m+1)$: Because $F(a) = 0$ we can write $F(x) := (x-a)B(x) \Rightarrow F'(x) = B(x) + (x-a)B'(x)$. Because $F'(a) = 0$, we can write $F'(x) := (x-a)(B_1(x) + B'(x))$ where $B(x) = (x-a)B_1(x)$. Now we have a function $F'(x)$ s.t $F^{(i+1)}(a) = 0$ for all $0 \leq i \leq m$, so a has zero multiplicity $m+1$. Therefore, for the function $F(x)$, a is a zero multiplicity of $m+2$. Hence, by induction, the claim holds for all m.

(b) $f(1) = 0$, $f'(1) = n1^{n-1} - n = 0$, $f''(1) = n(n-1)1^{n-1} = n(n-1) \neq= 0$, so 1 is a zero multiplicity of 2.

(Q-9) (a) $x^3 + a^2 + bx + c = 0 \Rightarrow x + a + \frac{b}{x} + \frac{c}{x^2} = 0$ if $x \neq 0$. None of $r, s, t = 0$ because $c \neq 0$ so

$$r + a + \frac{b}{r} + \frac{c}{r^2} = 0$$
$$s + a + \frac{b}{s} + \frac{c}{s^2} = 0$$
$$t + a + \frac{b}{t} + \frac{c}{t^2} = 0$$
$$r + s + t + 3a + b(\frac{rs + st + rt}{rst}) = c(\frac{1}{r^2} + \frac{1}{s^2} + \frac{1}{t^2}) = 0$$
$$\frac{b^2}{c^2} - \frac{2a}{c} = \frac{1}{r^2} + \frac{1}{s^2} + \frac{1}{t^2}$$

(b) $r+s+t=-a \Rightarrow r^2+s^2+t^2=a^2-2(rs+st+rt)=a^2-2b$
$rs+st+rt=b \Rightarrow r^2s^2+s^2t^2+r^2t^2=b^2-2rst(r+s+t)=b^2-2ac$
$rst=-c \Rightarrow r^2s^2t^2=c^2$
$x^3+(2b-a^2)x^2+(b^2-2ac)x-c^2$ will have root of r^2, s^2, t^2.

(Q-10) $ab^p-ba^p=ab(b^{p-1}-a^{p-1})$. It follows by Fermat's Little Theorem that $a^{p-1}\equiv 1 \mod (p)$ and $b^{p-1}\equiv 1 \mod (p)$. Thus, $p|(b^{p-1}-a^{p-1}) \Rightarrow p|ab^p-ba^p$.